[redacted]



25X1A2g

[redacted]

POLAND

MILITARY/AIR/NAVAL

Text of an Article: "Problems of the Efficiency of Secret Communications" by Major T. GRZYMALA

1. The lightning development of communications techniques, and the increase in the part played by manoeuvre and rapidity of action, have resulted in a situation where command is based to a considerable degree on technical means of signals communication. However, parallel with the increase in the importance of technical means of signals communication as a means of command, there is taking place the development of techniques of signals reconnaissance, and techniques of interception and exploitation of data transmitted by technical methods of signals communication. I consider that it will be useful to begin by discussing in some detail some of the problems concerning signals reconnaissance, and particularly its organisation in the U.S. Army.

2. Already during the First World War, the Director of the British Naval Intelligence, Reginald HALL, developed a system of monitoring German radio communications and of breaking their cyphers and codes. Also during the Second World War, U.S. Intelligence intercepted and broke Japanese coded signals [kodogram].

3. At the present time, the American Army possesses an extensively developed 'Communications Intelligence', subordinated to intelligence and reconnaissance organs, which is being carried out by an organisation called the 'Army Security Agency' (ASA). An ASA group is allocated from the Headquarters of the theatre of war operations to the field army, and operates for its benefit. The group consists of a Communications Reconnaissance Group (Com Ren Group), which in turn consists of Com Ren Battalions - one for each Army Corps - and a 'liaison team' - also one for each Division of the Corps. A Com Ren Bn probably contains two communications reconnaissance companies, which are the lowest organisational unit of the

/ASA .....



[redacted]

ASA adapted for the execution of independent tasks.

4. According to data obtained up to 1952 [sic], such a company covers with its operation an area 32-40 kms wide and 32 kms deep. The exploitation platoons of the company deploy at a distance of 2,700 metres from the FEBA, or sometimes at the FEBA itself. The company is able to operate 20 monitoring sets throughout the 24 hours. It may now be expected that there have been further improvements in signals reconnaissance equipment.

5. In general, the tasks of the ASA include, among other things, the acquisition of communications reconnaissance data by interception ..... [a line of text missing] ..... the maintenance of 'Communications Security' by own troops, and the execution of other tasks connected with communications reconnaissance and the organisation of secret communications.

6. The Americans regard communications reconnaissance as one of the most important sources of information. According to American views, reconnaissance conducted with the help of technical means of communication is able to obtain the following information:

- determine the strength, composition, and numbering of enemy units;
- determine the location of units, command posts and rear installations;
- watch the regrouping of enemy forces along the front, and the approach of fresh forces from the depth;
- discover the plans and intentions of enemy forces.

7. These tasks are carried out by means of:

- radio DF-ing, leading to the determination of the deployment areas of headquarters and military units;
- interception of conversations transmitted en clair, and the breaking of enemy cyphers, codes and signals;
- analysis of the radio traffic forming part of the enemy communications network (studying the principles of the radio signals plan, the number of messages transmitted by radio, etc.).

8. The work of the ASA in the army, and of similar groups in the naval

/and .....

and air forces, is coordinated by the National Security Agency. This is one of the branches of the Department of Defence, operating under the supervision of the Office of Special Operations, which forms a part of the Department of Defence. The principal task of the Agency is to discover the codes and cyphers of foreign countries, to break them in order to use them for its own purposes, and to intercept conversations en clair.

9. From statements made by William Ch. MARTIN and Bernon F. MITCHELL, the former employees of the U.S. National Security Agency who asked for asylum in the Soviet Union in August 1960, it is known that the central institutions of the Agency are located in the Fort George H. MURD [sic], Maryland, about 25 miles north of Washington. The Agency employs about 10,000 persons, directed (in 1960) by General of the Air Force John A. SEMFORD. The network of radio monitoring stations which supply intelligence to the Agency covers the entire globe and consists of over 2,000 listening posts serviced by 5,000 military operators.

10. A large number of instruments intercept information transmitted by teleprinter. The basic function of the monitoring service is continued by American military radio stations. Some monitoring sub-units are located in ships and aircraft. The interception of cyphered and encoded messages, as well as those transmitted en clair, is practised in respect of almost all the countries of the world.

11. The organisation of the National Security Agency includes four basic directorates. One of these is the operational directorate, which receives the material obtained from monitoring, carries out the cryptographic analysis of these materials, and studies the data thus obtained. The operational directorate contains the following basic sections:

- the ADVA section: studies the government cypher systems and diplomatic codes of the Soviet Union;

- the DENS section: studies the cypher systems of the Soviet Army, and the cypher systems used within the USSR;

- the ACOM section: studies the codes and cypher systems of

/socialist.....

socialist countries in Asia;

- the ALLO section: studies the codes and cypher systems of the allies of the United States, of neutral countries, and of other socialist countries.

12. The above consideration of the radio intelligence methods used by the U.S. Armed Forces (and undoubtedly a similar intelligence system is organised by other NATO countries as well) indicates the very real danger of discovery of information classified as a military secret, transmitted by technical means of signals communication.

13. The importance of this problem follows from the fact that, during exercises in units which did not apply the principles of Secret Communications, checks have shown that en clair procedure was used for the transmission by radio of information of such importance that, during /genuine/ military operations, if the enemy succeeded in intercepting this information, he would have been able to take effective counter-measures.

14. The conduct of military operations with the employment of weapons of mass destruction indicates the need for an even stricter observance of military secrecy. The object here is to prevent the discovery of worth-while targets for enemy nuclear strikes, and the preservation of strict secrecy regarding one's own intentions to carry out nuclear strikes.

15. Before passing to the discussion of the main problem, I wish to devote a short time to the necessity for maintaining a simplified system of command. As is known, on a nuclear battlefield one demands a greater independence among subordinates in the command of troops. Subordinates should be given their tasks in a brief and concise form. Signals for co-operation and simple signals taken from the signals table should form (in addition to the combat tasks) the basis for directing the operations by troops.

16. It is also unacceptable to permit the method, frequently employed during exercises, of the excessively frequent interference of superiors into the conduct /dynamika/ of combat, and of demanding reports on the situation

/of the .....

of the forces every one or two hours. Such a method of command results in the commanders (particularly unit commanders) becoming so absorbed in the preparation of reports that little time is left to them to the business of command. In addition, the prolonged period of operation of radio sets facilitates for the enemy the execution of DF-ing and the interception of certain important data. The employment of brief signals would, in my opinion, greatly hinder such action by the enemy.

17. The preparation of numerous documents during command (which is often done during exercises, simply in order to make an impression on the umpires) also has an adverse effect on the efficiency of command.

18. I should also like to draw attention to the importance and necessity of adhering, during the work of headquarters during exercises, to the principle that every soldier should have access only to those data which are necessary to him for the execution of his official duties. I make bold to say that in the majority of our exercises these principles are not followed. For instance, the preparations for an offensive (defensive) operation are known in the majority of cases, during exercises, to clerks, draughtsmen, drivers, etc., to whom this knowledge is completely unnecessary for their work. During war operations, when the enemy is conducting a vigorous reconnaissance, such a practice may have serious consequences.

19. I shall now discuss the, in my view, basic problems concerning secret communications. It will be realised that, within the framework of perfecting the system of command, the <u>increase in the efficiency of secret communications</u> is of capital importance.

20. It is obvious that a radical solution of the problem of secret communications could be found in the provision of technical means for concealment, such as cyphering machines, cyphering attachments to radio sets, and similar methods of scrambling conversation. However, the problem must be considered in the light of the existing situation in our armed forces. Until the problem is solved on an overall scale, it will be necessary to organise secret communications and to seek methods for its improvement within the

/limits.....

limits of our actual possibilities.

21. One of the important problems is the question of the organisation of secret communications already during peace-time, and the preparation of a cadre for its suitable employment during a war. It must be admitted that, in peace-time, the transmission of secret and confidential correspondence by technical means of signals communication (with the exception of cyphered correspondence) is very small, since almost all the official business is conducted by means of postal correspondence. Such a method greatly hinders the effective work of headquarters.

22. The number of transmitted letters is often so large that it actually hinders command. For instance, some regiments received during a year about 2,700 secret and confidential documents, not counting unclassified letters, which are often much more numerous. I should like only to indicate here the possibility of a partial solution of this problem by sending secret and confidential correspondence by means of coded signals /kodogram/, and overt correspondence by means of telegrams /telephonegram/, limiting the number of written correspondence to an essential minimum.

23. Such a solution of this problem will be of enormous value, for two reasons. Firstly, the style of work of headquarters will approximate to wartime conditions, when there will not be enough time to write many letters. Secondly, it will enable the officers (regular NCOs) to develop a habit of applying the principles of secret communications, so necessary in time of war. It is difficult to imagine that secret communications will be properly used during combat operations if they are completely disregarded in peace-time.

24. In military units from unit (independent sub-unit) upwards, the running of coding points should be entrusted to two officers or regular NCOs each (two, on account of possible departures, leave, etc.). For training purposes, the personnel running the coding points may be changed from time to time. Depending on local conditions of the unit concerned, the coding may also be performed by duty officers.

25. I also consider it useful to carry out a regular programme of

/training.....

training in Secret Communications for officers and regular NCOs, including in it some subjects concerning secret office routine. Such training should be conducted in accordance with a programme, and not organised ad hoc, depending for example on the results of a check, or on future examinations. Depending on the level of command, the programme should include a few hours devoted to theory, but most time should be devoted to practical work with secret communications documents. Practical work should be combined with the training of the cadre in the use of technical means of communication.

26. A subject of equal importance is the quality of the secret communications documents being prepared. It is obvious that combat documents drawn up during modern combat operations should be simple and easy to use. The difficulty lies in the fact that they must at the same time be proof against code-breaking. The quality of secret communications documents is above all influenced by the cyphering systems and the terminology.

27. One frequently meets with coding tables containing a large number of terms (500 to 1000 sentences and words), set up in the shape of phrases /? - rozwrot/, sectors, columns, and lines, provided of necessity with a complicated key system. Speaking from experience, I consider that using these tables is a difficult matter and that the efficiency in using them is very low. The coding officer spends most of his time in finding the required terms, rather than in coding. Obviously, the preparation of a "perfect" coding table is a very difficult matter, and there may be several different types of them. As a possible method of increasing efficiency in the sending of coded messages, I suggest the use of a coding table which is somewhat different from the one at present in use. This table would consist of a total of 200 entries, 100 of which would cover single letters and syllables, and the other 100 some generally-used words and phrases. Particular phrases may be permanently numbered, which will greatly increase efficiency since the codists will after a time know these numbers by heart. In order to provide a further safeguard against breaking the code, the text

/encoded.....

encoded in this way should be encoded a second time, by means of a special key. It is true that this will mean double coding but practical tests carried out in the Warsaw Military District indicate that coding by means of such a table is several times faster than when using tables with large numbers of terms.

28. Practical experience has shown that an excessively large number of terms contained in signal tables also greatly reduces the speed in using them (by reason of the time necessary to find the required words or phrases). Signal tables should be of small dimensions (so they could be put into a map-case) and contain the minimum number of terms needed for efficient operation. The preparation of such a table should be simple. The officer would enter in it the signals and data from secret communications documents needed by him, such as code-names, and signals for co-operation or passing information. The topographical code should be included in the terminology of the signal table and should be provided with numbering (not agreed words) which will facilitate its use. The possession of all the secret communications documents will greatly facilitate the work for the officers. In order to facilitate the direct transmission of data, the secret communications documents (with the exception of the coding table) may be prepared in such a way that the designations in each of them will have a different set of numbers, for instance, a signals table will use three-digit numbers, a map code four-digit numbers, etc.

29. The quality of the secret communications documents is determined by the terminology contained in them. It would seem best that in all the military units, headquarters, directorates /szefostwo/ of arms and services, and quartermaster HQs of the larger units, there should be prepared a terminology for coding and signal tables which would be different for peace-time use, different for wartime, and different again for exercises. The latter one should be known to all officers and regular NCOs employed in various headquarter sections. This terminology, used in coding and signal tables, should be perfected during exercises.



/30. .....

30. The preparation and possession in headquarters of a suitable terminology will make it possible to draft concisely the coded messages /kodogram/ and the contents of signals, which will greatly accelerate the transmission of coded messages and signals.

31. A separate problem is the matter of simplifying the records and documents of the coding point (coding table operating point). I regard the possibility of reducing the quantity of the documents being prepared as a partial solution of this problem which may also have influence on the increase in the efficiency of operation of the coding point. The object here is to eliminate from the coding folder such documents as the 'action register' /Dziennik Wykonawczy/, and the coding documents issue and receipt register. Entries concerning the registering of coding point documents, and of their issue and receipt, may be carried out on special sheets in the coded messages in-and-out-register.

32. It is also necessary to discuss the organisation and employment of secret communications during exercises.

33. During the preparatory period, the more important documents concerning the intentions of the operation (combat) will undoubtedly be passed on by personal contact between commanders or Staff officers, possibly in cypher. The remainder will be transmitted with the help of coding tables.

34. During actual combat, the majority of the data will be passed by means of signal tables and other agreed secret communications signs. Some data, however, requiring longer periods of validity will be transmitted by means of coding tables. I should like to stress here the possibility of increasing the efficiency of secret communications by using operational (general) signal tables in the individual communications networks of directorates of arms and services and in quartermaster headquarters, in addition to using the special tables of the various services. This will make possible a general exchange of information. Wider use than at present should be made of such secret communications agreed signals as: the numbering of crossing points (lines); points along assault routes; localities, etc.

/35. .....

35. It follows from the above that, during the preparatory period and in course of combat, a part of the data will be transmitted by means of coding points, and the remainder by officers. For this reason the proper organisation of coding points in units becomes of considerable importance since it is on them that the practical employment of secret communications will largely depend. In connection with this, it is my opinion that an establishment should be provided, for the time of war, for coding NCOs in independent units of the army, in units and some independent sub-units of the division, and even in the more important units and directorates of arms and services of the army command. I support this argument by the fact that the detailing for coding of an officer /already/ fulfilling a specified function will not increase the efficiency of secret communications.

36. In peace-time the yard-stick for checking the proper application of principles of secret communications is provided by exercises. I consider that in future greater attention should be paid to the proper and real checking of secret communications during exercises. The check should consist of demonstrating to the personnel engaged in the exercise the dangers resulting from the exposure of military secrets. The leadership of the exercise, or the umpires, should immediately react to every case of the exposure of military secrets by the participants in the exercise, creating situations approximating to a real one. Such checking during exercises would present to the participants a realistic picture of the dangers resulting from the exposure of secret data to the enemy.

CONTROLLED DISSEM
NO FOREIGN DISSEM
BACKGROUND USE ONLY
no dissem abroad